Exhibit 3

KAISERDILLON PLLC

1099 14TH ST. NW
8TH FLOOR WEST
WASHINGTON, DC 20005
(202) 640-2850
WWW.KAISERDILLON.COM

January 22, 2021

VIA ELECTRONIC MAIL
Mr. Jay Prabhu
Mr. William G. Clayman
Assistant United States Attorneys
United States Attorney's Office for the Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Jay.Prabhu@usdoj.gov
William.G.Clayman@usdoj.gov

Re: *United States v. Zackary Ellis Sanders*, 1:20-cr-00143

Dear Jay and Bill,

We write regarding discovery and our continuing concerns over the Government's compliance with its obligations. Specifically, now that we understand from our own investigation that the search warrant for the Sanders' family home was obtained as part of a nationwide investigation that relied on form affidavits—facts both the defense and the Court should have learned from the Government much earlier—there are certain additional discovery materials to which Mr. Sanders is entitled, as set forth below. In addition, we reiterate our previous requests for the screenshot the Government continues to withhold of the "Register" page from [redacted], which is referenced in Paragraph 18 of Special Agent Ford's Affidavit.

The Nationwide Scope of the FBI's Operation

As discussed in Mr. Sanders's Motion to Modify the Protective Order filed under seal yesterday (ECF Nos. 229, 230, 234), the defense is now aware, from its own investigation, that Mr. Sanders's case was part of a sweeping FBI operation that was nationwide in scope. *See, e.g.,* [redacted]

[redacted]; ECF No. 43 (explaining affidavit in support of the search warrant describes the [redacted]); [redacted][1]

Given the scope of the FBI's operation, we believe that it corresponds with [redacted] and mirrors the "Playpen" operation, a.k.a., "Operation Pacifier." Like Operation Pacifier, this appears to be a nationally coordinated investigation where FBI agents were directed to use template affidavits to obtain search warrants and to conceal and minimize the international scope of the investigation. *See* Exhibits A (Template Affidavit from Operation Pacifier) and B (Internal FBI Email Regarding Operation Pacifier). The principal difference between this operation and Operation Pacifier appears to be that, whereas in Operation Pacifier the FBI itself deployed Network Investigative Techniques (NITs), here the FBI relied on the [redacted] to do so, with the use of [redacted], in order to evade the Fourth Amendment requirement of first applying successfully for a warrant.

Based on the above, Mr. Sanders is requesting further discovery related to the Affidavit in Support of the Search Warrant, Mr. Sanders's subsequent Motions to Suppress, and the Government's Rule 414 Notices.

[1] The apparent scope of the operation runs contrary to the Government's representations to the Court in this case. The Government's representations have incorrectly suggested that the FLA was supplying information about one IP address, when it was in fact generalizing about the purported activity of many IP addresses provided by the FLA. For example, the Government has stated:

- "[redacted]." ECF No. 43 at 1 (emphasis added).
- "[redacted]" ECF No. 70 at 2 n.1 (emphasis added).

First, Mr. Sanders requests the template affidavit that Special Agent Ford relied on to draft the Affidavit in this case, and which FBI agents have relied on to draft affidavits in other cases related to [redacted]. *See, e.g.,* Exhibit A. This template affidavit would demonstrate that the allegations contained in Special Agent Ford's Affidavit were generic and not specific to Mr. Sanders (other than connecting a specific IP address to a specific physical address and its occupants); that there was no effort to corroborate the FLA's tip; that this was a bulk operation that was meant to describe the activities of a large number of individuals and not any activity or characteristics of Mr. Sanders specifically; and that there was no evidence of Mr. Sanders's activity on the website, as Paragraph 23 of the Affidavit clearly suggested there was.

Second, we are requesting the number of IP addresses that the FLA provided to the FBI under i) [redacted] and ii) [redacted]; the number of IP addresses that the FBI sought search warrants for; and the number of searches that did not lead to child pornography-related charges being filed.

Third, we request additional reports relating to this Operation and its case developments, including from the Major Case Coordination Unit and the Assistant Director Case of Interest reports. These reports would include points of contact for the operation, significant activity, background information, future planned activities, and strategy (including in response to defense motions)—all of which are material to Mr. Sanders's motions to suppress. For example, these documents would demonstrate that [redacted] involved more than one Tor Onion Service website, that the FBI had no evidence of Mr. Sanders's specific activity online (whether that was on Tor or any other application), that the FBI had no evidence that the content that Mr. Sanders purportedly accessed met the definition of child pornography under U.S. law, and that the Government is seeking to conceal such information from the defense and from courts.

The Register Screenshot

The Government's late disclosure of two innocuous, exculpatory screenshots of the target website reveals that the Government is continuing to withhold at least a third screenshot: the "Register" page referenced in Paragraph 18 of Special Agent Ford's Affidavit. We believe that this screenshot is also in the Government's possession, custody, or control and also reflects that even if an Internet user went deeper into the website, the page for registering an account does not advertise, display, or allude to illegal content.

* * *

Please provide any documents, material, or information related to the categories and questions above by February 1, 2021. We believe that the information and documents we are requesting are in the Government's possession, custody, or control and are material to preparing

Mr. Sanders's defense.[2] If you decline to produce the requested information, please let us know by January 25, 2021, so we can seek appropriate relief from the Court.

Thank you in advance for your courtesy.

Sincerely,

Jonathan Jeffress
Counsel for Zackary Ellis Sanders

[2] *See* Fed. R. Crim. Pro. 16(a) (requiring the Government to permit inspection of certain records, "if those records are in the government's custody and the item is material to preparing the defense."); *see also United States v. Salad*, No. 2:11CR34, 2012 WL 5894387, at *1 (E.D. Va. Nov. 23, 2012).

Exhibit A

AFFIDAVIT OF [NAME]
IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, [name], being first duly sworn, hereby depose and state as follows:

A. Introduction and Affiant Background

1. I make this affidavit in support of an application for a search warrant to use a network investigative technique ("NIT"). I request approval to send one or more communications to [address]. Each such communication is designed to cause the computer receiving it to transmit data that will help identify the computer, its location, other information about the computer, and the user of the computer. As set forth herein, there is probable cause to believe that violations of Section [crime] of Title 18, United States Code ([crime]) have occurred and that evidence of those violations exists on the computer that receives the NIT described above.

2. [agent background]

3. [**USE ALL THAT APPLY** - The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.] Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

B. Probable Cause

4. [explain why probable cause exists to believe that a NIT sent to the address will reveal evidence, such as how the computer expected to receive the NIT was used in the commission of a crime or how identifying the computer or account user is evidence of who committed the crime under investigation.]

C. Place to be Searched and Property to be Seized

5. If a computer successfully activates the NIT, the NIT will conduct a one-time limited search of that computer. The NIT utilizes computer instructions to cause an activating computer to send certain information to a computer controlled by the [server owner, typically the investigating agency].

6. The NIT is designed to collect the items described in Attachment B – *i.e.*, information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section [crime] of Title 18, United States Code ([crime]). This information may include the portion of the activating computer that contains environmental variables and/or certain registry-type information, such as:

A. The computer's IP address. An IP Address is a unique numeric address used to direct information over the Internet and is written as a series of four numbers, each in the range 0 – 255, separated by periods (e.g., 121.56.97.178). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

B. The computer's MAC address. Each time a computer communicates over a local area network (or "LAN"), it uses a hardware device called a network interface card. Manufacturers of network interface cards assign each one a unique numeric identifier called a media access control or "MAC address."

C. The computer's open communication ports. A communication port number is information that helps computers to associate a communication with a particular program or software process running on a computer efficiently. For example, if a communication is sent to port 80, the receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.

D. A list of running programs running on the computer.

E. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Vista), and serial number.

F. The web browser and version running on the computer. The web browser is the program that allows user to view web pages. Firefox, Internet Explorer, Netscape, Opera and Safari are examples of web browsers.

G. The computer's language encoding and default language. Users can set computers to display text in a particular language.

H. The computer's time zone information.

I. The registered computer name and registered company name. Users generally input this information when the computer is first purchased.

J. The current logged-in user name and list of user accounts.

K. The computer's wired and wireless network connection information, dial-up account information, and trace-route information. This information identifies the way that the computer is connected to the Internet.

L. Uniform Resource Locator ("URL") to which the target computer was previously connected. URLs, such as www.uscourts.gov, are used to access web sites.

M. Other similar information on the activating computer that may assist in identifying the computer, its location, other information about the computer, and the user of the computer may also be accessed by the NIT.

7. Each of these categories of information sought by the NIT may contain evidence of the crime under investigation, including information that may help to identify the computer receiving the NIT and its user. The computer's true assigned IP address can be associated with an Internet service provider ("ISP") and a particular ISP customer. The MAC address is unique to a specific computer on a network. A list of open communication ports and running programs can corroborate whether the NIT is reading the correct computer by showing whether that computer is using the world wide web, sending and receiving emails, or reading attachments. The operating system and browser types and versions can also corroborate the identity of a computer and, in the case of an

operating system's serial number, can provide evidence to identify the user because corporations maintain databases of purchasers of their operating systems. The language encoding and computer default language can help identify the subject by identifying his native spoken language. The computer name, company name, logged-in user name can identify the network, specific computer on a network, and perhaps even the name of the person(s) who use the computer. Traceroute information can help identify where on a network or even where physically a computer may be located. Wireless network connection information can tell from where a computer accessed the Internet, even if it was through the unauthorized use of a wireless network (a technique used by Internet criminals). Wired network information and dial-up account information can help identify what computer was used to access the Internet to receive the NIT. Time zone information will assist in confirming the geographical location of the subject computer. The last-visited URL can sometimes help corroborate the identity of the computer and user by, for example, showing that the NIT ran after the user visited the web-based e-mail server for the target email address.

8. Based on my training, experience, and the investigation described herein, I know that network level messages and information gathered directly from a sending computer can be more effective than other types of information in identifying a computer, its location and individual(s) using a computer. For instance, individual(s) using the Internet can use compromised computers or commercial services to conceal their true originating IP address and thereby intentionally inhibit their identification. Getting IP address and other information directly from the computer being used by the subject can defeat such techniques.

9. The NIT will cause the above-described information to be sent over the Internet to a computer controlled by [server owner, typically the investigating agency] located in [jurisdiction] [and then relayed to investigators in this District].

10. Based upon the information above, I have probable cause to believe that the computer that receives the NIT is [an instrumentality and contains evidence] of violations of Title 18, United States Code, Section [crime]. I further submit that there is probable cause to believe that using a NIT in conjunction with the target address will assist in identifying the activating computer, its location and the individual(s) using the activating computer to commit these violations of the United States Code. By this affidavit and application, I request that the Court issue a search warrant authorizing the use of the NIT described herein.

11. **[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]]**After the one-time search, the NIT will record routing, addressing and signaling information for electronic communications originating from the activating computer for 30 days. More specifically, the NIT may report the following types of information: IP address, MAC address, open communication ports, trace-route information, wireless network connection information, wired network connection information, dates, and times of the electronic communications, but not the contents of such communications. For a period of thirty days the NIT will forward that data to a computer controlled by the [server owner, typically the investigating agency.] Such information is relevant and material to the government's ongoing criminal investigation.

12. **[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]]** The routing, addressing and signaling information described in the preceding paragraph will help show the ordinary things that a pen register on the user's Internet connection would reveal, that is, with what Internet sites the user communicates. Such information can help reveal the user's techniques, interests, and associations, and thereby may assist in attributing to a particular person the use of the computer receiving the NIT. The routing and addressing information to be collected will show where and when the computer(s) access the Internet over that period, if it changes. Once the government knows the IP addresses from which it accesses the Internet, the government will be better able to determine the physical location of those IP addresses by using publicly available data or grand jury subpoenas. [additional grounds].

13. **[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]]**A separate application for the installation and use of a pen register and trap and trace device is also being sought for the use of the NIT.

14. Because notice as required by Rule 41(f)(3) of the Federal Rules of Criminal Procedure would jeopardize the success of the investigation, and because the investigation has not identified an appropriate person to whom such notice can be given, I hereby request authorization to delay such notice for 30 days from the sending of the NIT.

15. Because there are legitimate law enforcement interests that justify an unannounced use of the NIT and review of the messages generated by the activating

computer in this case, I ask this Court to authorize the proposed use of a NIT without the prior announcement of its use. One of these legitimate law enforcement interests is that announcing the use of the NIT would assist a person using the activating computer to defeat the activation of the NIT.

16. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that the warrant command the law enforcement officer (a) "to execute the warrant within a specified time no longer than 10 days" and (b) to "execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time . . . ." The government seeks permission to deploy the NIT at any time of day or night within 10 days of the date the warrant is authorized. There is good cause to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to anyone. The government also seeks to read any messages generated by the activating computer as a result of a NIT at any time of day or night during the execution of the warrant. This is because the individuals using the activating computer may activate the NIT after 10:00 PM or before 6:00 AM and law enforcement would seek to read the information it receives as soon as it is aware of the NIT response.

17. The government does not currently know the exact configuration of the computer that may be used to access the target address. Variations in configuration, e.g., different operating systems, may require the government to send the target address more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the target address for up to 10 days after this warrant is authorized, until the NIT has returned the information authorized to be collected by this warrant.

18. To the extent that use of a NIT to obtain the information described herein can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary for the reasons described herein.

19. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

A. the use of multiple communications until the NIT has returned the information authorized to be collected by this warrant, without prior announcement, within 10 days from the date this Court issues the requested warrant;

B. the NIT may cause an activating computer – wherever located – to send to the government in [location], [and thereafter to the government in this District,] network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer;

C. that the government may receive and read, at any time of day or night, within 10 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by the [server owner, typically the investigating agency];

D. **[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]]** that once the government has received an initial NIT response from the activating computer, the government may for 30 days thereafter collect dialing, routing addressing, and signaling information that can be collected pursuant to a pen register and trap and trace device order; and

E. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days from the sending of the NIT [or, in the case of a NIT with ongoing monitoring, 30 days after the termination of the pen/trap order] unless notification is further delayed by court order.

F. that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

20. I further request that this Application and the related documents be filed under seal. The information to be obtained is relevant to an on-going criminal investigation. Premature disclosure of this Application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of the technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.

WHEREFORE, Affiant respectfully requests that a warrant described above be issued.

____
[affiant]

Subscribed and sworn to me before me
this __________ day of _________, ______

____
HON. [judge]
U.S. Magistrate Judge

Attachment A

Place to Be Searched

The portion of the computer activating the NIT that may assist in identifying the computer, its location, other information about the computer, and the user of the computer.

Attachment B

Things To Be Seized

Information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section [crime] of Title 18, United States Code ([crime]).

Attachment C

IT IS ORDERED that the government is authorized to use multiple communications until the NIT has returned the information authorized to be collected by this warrant, without prior announcement, within 10 days from the date this Court issues the requested warrant;

IT IS ORDERED that the NIT may cause an activating computer – wherever located – to send to the government in [location], [and thereafter to the government in this District,] network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer;

[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]] IT IS ORDERED that once the government has received an initial NIT response from the activating computer, the government may for 30 days thereafter collect dialing, routing addressing, and signaling information that can be collected pursuant to a pen register and trap and trace device order; and

IT IS ORDERED that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

Exhibit B

From: [redacted]
Sent: Wednesday, January 20, 2016 1:27 PM
To: [redacted]
Subject: FW: Pacifier - Possible [redacted] Disclosures --- UNCLASSIFIED

b6 -1,3
b7C -1,3
b7E -7

```
Classification: UNCLASSIFIED
============================================================
```

Also [redacted] is out of the office today so he asked that I also forward this along....FYSA.

b6 -1
b7C -1

[redacted]

From: [redacted]
Sent: Thursday, January 14, 2016 8:30 AM
To: [redacted]
[redacted]
Subject: Pacifier - Possible [redacted] Disclosures --- UNCLASSIFIED

b6 -1,3
b7C -1,3
b7E -7

```
Classification: UNCLASSIFIED
============================================================
```

As a follow-up to my email last night, these are the following stats that could become public after the hearing on January 22 if the judge unseals the filings in the case:

[redacted]

b7E -2,3,7

The fact that we had mitigation procedures in place but no specifics on what those procedures were or whether or not they were activated.
The reason the site was shut down [redacted]

Things that have not been disclosed in any filings that we want to continue to protect to the best of our ability (I have made [redacted] aware of these items):
The scope of the international aspect of the investigation
The fact that we located/arrested administrators [redacted]
[redacted]

b6 -1,3
b7C -1,3
b7E -10

The only item from the above list that defense is already aware of is the fact that we arrested the main admin in Florida. That information is not reflected in any filings at this point but nothing is stopping them from putting it on paper in a future filing. The fact that two administrators of a [redacted] child porn website were arrested during the time of our operation is also reflected in local news stories that as of yet, nobody has tied to our case.

b6 -4
b7C -4
b7E -3

SA [redacted]

[redacted]

b6 -1
b7C -1
b7E -8

==
Classification: UNCLASSIFIED

==
Classification: UNCLASSIFIED

==
Classification: UNCLASSIFIED